

Chapter 3: Kerberos Principals and Passwords

In this chapter we discuss choosing and obtaining a strengthened realm userid (called a *Kerberos principal*) and a Kerberos password.

3.1 Your Kerberos Principal

As a user, you need to obtain a Kerberos Principal¹ (actually one for each realm, FNAL.GOV and FERMI.WIN.FNAL.GOV), in order to access machines and resources at Fermilab. A principal is essentially a username for the strengthened realm. Your principals will have the same username, and be of the form `principal_name@REALM` (e.g., `jpe@FNAL.GOV` and `jpe@FERMI.WIN.FNAL.GOV`). You must have a valid Fermilab ID.

In addition to a principal, you must have an account on each machine that you plan to use in the realm. There are significant conveniences if your principal and your account name are the same, as we discuss in section 3.1.1 *Choosing a Principal Name*.

The system administrator of a strengthened machine may require that authorized users obtain a `<username>/root` instance of their Kerberos principal in order to access sensitive accounts on the system. The root instance has tighter restrictions placed on it (see section 9.2 *Ticket Management*). If your system administrator tells you it's required, use the form *Request Additional Kerberos Items* at

http://computing.fnal.gov/cd/forms/extra_kerb_req_form.html.

1. Note for sysadmins: if you have an account and a standard UNIX password (in the `passwd` file or NIS map) on a Kerberized machine, but no principal or Kerberos password, you can still log in and use non-Kerberized services. You can do this only at the console. (From any other terminal, the Kerberized system responds in portal mode, described in section 4.4 *Connecting from a NonKerberized Machine: Portal Mode*, and you have no option to enter your UNIX password.)

3.1.1 Choosing a Principal Name

The Kerberos Strong Authentication system includes virtually all computer systems across the site. Your Kerberos principal will be used for authentication sitewide. It is to your benefit to have one login id (account name) common to all systems that you use, and for that login id to match your Kerberos principal. The Computing Division is strongly encouraging this practice for ease of use, and in fact is enforcing it for new users. Keep in mind that the principal name you choose will be your permanent ID at Fermilab. Here are guidelines for choosing the name you'll use for your Kerberos principal:

New principals must be chosen to be eight (8) or fewer characters. Please use only lowercase letters and digits 0 through 9. **Do not use any uppercase letters or any special characters.**

In Appendix C: *More about Choosing a Principal Name*, we present information for users who have pre-existing account names and/or an email address at Fermilab, and for whom the above guidelines are not straightforward to follow.

3.1.2 Requesting a Principal

Use the online *Request Form for Computing Username and Primary Accounts* at http://computing.fnal.gov/cd/forms/acctreq_form.html.

3.2 About Kerberos Passwords

Once your request for a principal has been approved, you must stop by Wilson Hall, ground floor, north (the CD Help Desk) to receive your initial Kerberos password. An exception is granted for off-site visitors: you can get it over the telephone (630-840-2345); you will be asked a question to verify your identity.

You are required to change the initial password within 30 days of receipt, and once a year (actually every 400 days) thereafter.

Even if you use a CRYPTOCARD exclusively, you need to change your Kerberos password as stated above in order to continue accessing machines in the FNAL.GOV realm! If your password expires, you can still change it as long as you remember what it was, but you cannot use CRYPTOCARD access while it remains expired.



3.2.1 Important! Please Read!



Please treat your Kerberos password as an inviolable object. Never give your password to anybody for any reason. Doing so constitutes a policy violation. If you really need to give someone access to your account (this practice is discouraged, by the way), add the person's principal to your `.k5login` or `.k5users` file as described in section 9.3 *Account Access by Multiple Users*.

Typing in your Kerberos password should ideally be done infrequently (i.e., no more than once each day). Do not type it in carelessly. Please authenticate locally and forward your credentials to remote systems.

Windows 2000 domain-only users: type your password **only** at the Windows login prompt.

3.2.2 Choosing a Kerberos Password

In contrast to the principal (which ideally should match your login name on each machine and your email address), your Kerberos password must be unique. That is, in order to avoid exposing your Kerberos password, it must be different from the passwords you use for any other purpose (with the single exception that you may use the same one for both strengthened realms at Fermilab).

The Fermilab Computer Security Team has imposed some restrictions on passwords in accordance with DOE guidelines. Currently, a password for the FNAL.GOV strengthened realm is required to contain a minimum of ten characters from at least two of the following five classes: lowercase letters, uppercase letters, numbers, punctuation, and all other characters. Passwords for /root principals must contain a minimum of 11 characters including at least three of the five classes. Passwords the system considers “bad” will be rejected. (Passwords are checked against the “cracklib” dictionary, which will often surprise you by its thoroughness!)



Choose something that's hard to guess but that you can remember, and please make an effort to remember it!!

Need some ideas for thinking up a good password?¹ Remember, a good password is one you can remember, but that no one else can easily guess. Examples of passwords that would be good *if they weren't listed in this manual* include:

- some initials, like “GykoR66.” for “Get your kicks on Route 66.”
- an easy-to-pronounce nonsense word, like “slaRooBey” or “krangits”
- a misspelled phrase, like “2HotPeetzas!” or “ItzAGurl!!!”

1. These ideas were lifted from MIT's Kerberos V5 User's Guide (C) 1996, at (new link) <http://hoth.stsci.edu/public/krb5/user-guide.html>.



Note: Don't actually use any of the above passwords. They're only meant to show you how to make up a good password. Passwords that appear in a manual are the first ones intruders will try.

3.3 Changing your Kerberos Password

A few notes before moving to the platform-specific instructions:

- If you forget your initial password before you get around to changing it, open a helpdesk ticket requesting a password reset. Go to <http://helpdesk.fnal.gov/>.
- Change your password on a machine that is sitting in front of you and that has Kerberos or Reflection or other Kerberos-aware program installed. Do not send your password over a network connection to a remote host!
- The Computing Division has set up a terminal at which people can change their Kerberos passwords. It is in the CD Helpdesk/Email Center in Wilson Hall, ground floor, north end. Signage is mounted on the wall above the screen with instructions.
- If you don't have an appropriate machine on which to change your password, find someone who does, and borrow his or her command prompt. (Yes, you can change it from someone else's account; just give your principal name as an argument. For Reflection, add your principal into your colleague's configuration.) Or you can install a simpler, client-only version of Kerberos on your local machine; see section 6.2 *In a Pinch: Download Client-Only Version of Kerberos*.
- If your only option is to change it on a remote host via a network connection, then before changing your password, **verify that you are using an encrypted connection!** How do you know if your connection is encrypted? See Chapter 11: *Encrypted vs. Unencrypted Connections* for some help.

3.3.1 UNIX/Linux/Cygwin

To change your password, run the **kpasswd** command locally on your desktop or laptop.

The **kinit** program warns you if your password is within 30 days of its expiration date, and as of **kerberos** v1_2, the **kerberos** login program includes this warning as well.



On strengthened UNIX systems running AFS, there are two **kpasswd** commands, one for AFS (`/usr/afsws/bin/kpasswd`) and one for Kerberos (`/usr/krb5/bin/kpasswd`). Your `$PATH` should be set such

that the Kerberos **kpasswd** comes first. Kerberos is implemented at Fermilab such that your AFS tokens will be obtained automatically along with Kerberos tickets. If you are unsure which **kpasswd** is being invoked, force the system to use the Kerberos version by running **setup kerberos** first.

```
% setup kerberos
```

Then run **kpasswd**. If borrowing someone else's account or if your principal does not match your login id, include your principal name as an argument.

```
% kpasswd [<principal_name>]
```

```
kpasswd: Changing password for aheavey@FNAL.GOV.
Old password:                <--- type your initial password here.
kpasswd: aheavey@FNAL.GOV's password is controlled by the policy default,
which
requires a minimum of 10 characters from at least 2 classes (the five classes
are lowercase, uppercase, numbers, punctuation, and all other characters).
New password:                <--- type your new password here.
New password (again):        <--- type your new password here for confirmation.
Kerberos password changed.
```

If you choose a password that is too short, you will see this error message:

```
kpasswd: New password is too short.
Please choose a password which is at least 10 characters long.
```

If it's long enough but you haven't met the multiple-class requirement, you'll see:

```
kpasswd: New password does not have enough character classes.
The character classes are:
- lower-case letters,
- upper-case letters,
- digits,
- punctuation, and
- all other characters (e.g., control characters).
Please choose a password with at least 2 character classes.
```

If the password has expired, you'll need to get access to a machine running **kpasswd** some other way (e.g., find a friend or use a local account) to change it.

3.3.2 Windows (with WRQ® Reflection software installed)

Here we assume you are running the **WRQ® Reflection** software for **Windows** as described in Chapter 19: *Installing and Configuring WRQ® Reflection on a Windows System*.

To change your Kerberos password via the **Reflection** application, navigate to **START > PROGRAMS > REFLECTION > UTILITIES > KERBEROS MANAGER** to open the **Reflection Kerberos Manager** application. From the **TOOLS** menu select **CHANGE PASSWORD...** and change it. The password you enter does not go across the network; this is safe. Wait a few seconds for a message to appear indicating that it's been successfully changed.


If it doesn't work, try updating the Windows services file by executing `\\Pckits\WRQ\services.bat`. For Win95 or 98, you must copy it manually from `\\Pckits\WRQ\` (target directory may vary). This file is typically updated during installation of Reflection, so shouldn't normally be required at this stage.

3.3.3 Windows (with Exceed 7.0 and MIT Kerberos)

Here we assume you are running **Exceed 7** with the **MIT Kerberos** software for Windows as described in Chapter 21: *Installing MIT Kerberos on Windows, for use with Exceed 7 and FileZilla*.

Leash32 found in the **MIT Kerberos 2.5** or later (for Windows) can be used to change the password for an MIT Kerberos principal. To change your password:

- Navigate to **START > PROGRAMS > KERBEROS UTILITIES > LEASH32**.
- On the **Leash32** window, go to the **ACTIONS** menu and select **CHANGE PASSWORD**, and follow the instructions.

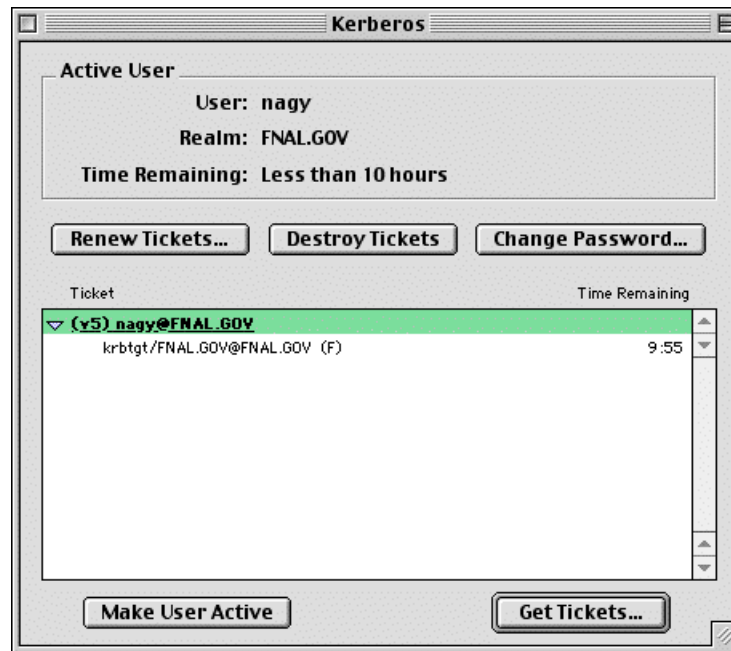
 In earlier versions, the **CHANGE PASSWORD** utility in **Leash32** does not work, and **kpasswd** in the Command Prompt works for the AFS password. For these earlier versions, then, changing your password under this configuration requires typing your password over a network connection. Please upgrade, or try to find a machine on which you can change your password locally, instead.

3.3.4 Macintosh

Here we assume you are running the **MIT Kerberos** software for Macintosh as described in Chapter 23: *Installing and Configuring MIT Kerberos on a Macintosh System*. To change your Kerberos password on OS X, either use **kpasswd** at the command line as in Unix, or the Change Password button on the GUI. For OS 9 and earlier:

- 1) Invoke the **Kerberos Control Panel** (from **CONTROL PANELS** under the Apple menu, from the **KERBEROS MENU** in the menu bar, or from the

KERBEROS CONTROL STRIP module).



- 2) Select a username and realm and click **GET TICKETS** for which you will have to provide your current (or initial) Kerberos password.
- 3) Click on the ticket to highlight it, then click **CHANGE PASSWORD** and enter the old and new passwords on the pop-up screen which appears.

